A generalized artihmetic geometric mean

Carls, Robert

Chapter 4

A theta structure induced by a lift of relative Frobenius

The main result of the present chapter is given by Theorem 4.1.1 which states the existence of a certain theta structure induced by the relative Frobenius. We remark that a theta structure for an abelian scheme with a given relatively ample line bundle induces a projective embedding of the abelian scheme. Thus Theorem 4.1.1 is an important step towards explicit coordinates for the GAGM sequence in higher dimensions (compare Section 1.3).

Structure of Chapter 4:	
Section 4.1:	We state our main theorem about the existence of a certain theta structure induced by a lift of the relative Frobenius.
Section 4.2:	Some general remarks are made about the notation that we will use in this chapter.
Section 4.3:	We provide some facts about theta groups and theta structures that we will need later on.
Section 4.4:	We state two theorems about the descent of line bundles along lifts of the relative Frobenius and the Verschiebung which are used in the proof of Theorem 4.1.1.
Section 4.5:	We give proofs of the statements made in the preceding sections.
Acknowledgments	
Bibliography	

4.1 The main result

Let R be a complete noetherian local ring with perfect residue class field k of characteristic $p > 0$ and A an abelian scheme over R of relative dimension g having ordinary reduction. Let $\mathcal{L}$ be an ample line bundle of degree 1 on A.

The following is a short exposition of some facts that will be discussed in detail in Section 4.4. There exists an isogeny of abelian schemes $F : A \to A^{(p)}$, which is uniquely determined up to isomorphism by the condition that it lifts the relative p-Frobenius on the special fiber. Also there exists an ample line bundle $\mathcal{L}^{(p)}$ of degree 1 on $A^{(p)}$ such that $F^*\mathcal{L}^{(p)} \cong \mathcal{L}^{\otimes p}$. It is uniquely determined up to isomorphism by the condition that $\left(\mathcal{L}^{(p)}\right)_k \cong \mathrm{pr}^*\mathcal{L}_k$, where $\mathrm{pr} : A_k^{(p)} \to A_k$ is an isomorphism making the diagram

$$\begin{tikzcd} A_k^{(p)} \arrow[r, "\mathrm{pr}"] \arrow[d] & A_k \arrow[d] \\ \mathrm{Spec}(k) \arrow[r, "f_p"] & \mathrm{Spec}(k) \end{tikzcd}$$

cartesian. Here f_p denotes the morphism induced by the absolute p-Frobenius of the field k and the vertical arrows are the structure morphisms. Assume that we have an isomorphism

$$(\mathbb{Z}/p\mathbb{Z})_k^g \xrightarrow{\sim} A_k[p]^{\mathrm{et}} \tag{4.1}$$

where $A_k[p]^{\mathrm{et}}$ denotes the maximal étale quotient of $A_k[p]$ (compare Section 2.9). The following is the main result of the present chapter.

Theorem 4.1.1 *Suppose $p > 2$. Then there exists a natural theta structure of type $(\mathbb{Z}/p\mathbb{Z})_R^g$ for the pair*

$$\left(A^{(p)}, \left(\mathcal{L}^{(p)}\right)^{\otimes p}\right)$$

depending on the isomorphism (4.1).

For a definition of a theta structure we refer to Section 4.3.3.

Corollary 4.1.2 *Let k be a finite field of characteristic $p > 2$. Assume that A is the canonical lift of A_k. Then there exists a natural theta structure of type $(\mathbb{Z}/p\mathbb{Z})_R^g$ for the pair*

$$\left(A, \mathcal{L}^{\otimes p}\right)$$

depending on the isomorphism (4.1).

Theorem 4.1.1 and Corollary 4.1.2 will be proven in Section 4.5.3.

4.2 Notation

Let R be a ring, X an R-scheme and S an R-algebra. By X_S we denote the base extended scheme $X \times_R \mathrm{Spec}(S)$. Let $\mathcal{M}$ be a sheaf on X. Then we denote by $\mathcal{M}_S$ the sheaf that one gets by pulling back via the projection $X_S \to X$. Let $I : X \to Y$ be a morphism of R-schemes. Then I_S denotes the morphism that is induced by I via base extension with S. We use the same symbol for a scheme and the fppf-sheaf represented by it. By a *group* we mean a group object in the category of fppf-sheaves. If a representing object has the property of being finite (resp. flat, étale, connected, etc.) then we simply say that it is a finite (resp. flat, étale, connected, etc.) group. Similarly we will say that a morphism of groups is finite (resp. faithfully flat, smooth, etc.) if the groups are representable and the induced morphism of schemes has the corresponding property.

A group resp. a morphism of groups is called finite locally free if it is finite flat and of finite presentation. The Cartier dual of a finite locally free commutative group G will be denoted by G^D. The multiplication by an integer $n \in \mathbb{Z}$ on G will be denoted by $[n]_G$ or simply $[n]$. A finite locally free and surjective morphism between groups is called an *isogeny*. By an *elliptic curve* we mean an abelian scheme of relative dimension 1. We use the notion of a *torsor* in the sense of [DG70] Ch. III, §4, Def. 1.3. We only consider torsors for the fppf-topology.

4.3 Theta groups

In the following section we recall some well-known facts about theta groups. We refer to [Mum66], [Mum70] Ch. IV, §23 and [MB85] Ch. V for more details. Let R be a ring and G a group over R.

Definition 4.3.1 *Assume that there exists a central exact sequence of groups*

$$0 \to \mathbb{G}_{m,R} \to G \xrightarrow{\pi} H \to 0,$$

where H is a commutative finite locally free group whose rank is the square of an integer. Then the group G is called a theta group *over H.*

By the term *central exact sequence* we mean that $\mathbb{G}_{m,R}$ is mapped into the center of G. Now let G be a theta group over H. By definition G is a $\mathbb{G}_{m,R}$-torsor over H. It follows by descent that the group G is representable by an affine faithfully flat group scheme of finite presentation over H (compare

[DG70] Ch. III, §4, Prop. 1.9). Let S be an R-algebra. One defines the *commutator pairing*

$$e : H \times_R H \to \mathbb{G}_{m,R}$$

by lifting x resp. y in $H(S)$ to $\tilde{x}$ resp. $\tilde{y}$ in $G(S')$, where $S \to S'$ is an fppf-extension, and by setting

$$e(x,y) = \tilde{x}\tilde{y}\tilde{x}^{-1}\tilde{y}^{-1}.$$

Because H is abelian, we have $e(x,y) \in \mathbb{G}_{m,R}(S')$. Since $e(x,y)$ does not depend on the choice of $\tilde{x}$ and $\tilde{y}$, it follows by descent that $e(x,y) \in \mathbb{G}_{m,R}(S)$.

4.3.1 The theta group of an ample line bundle

Next we give a first example of a theta group. Let A be an abelian scheme over a ring R and $\mathcal{L}$ a line bundle on A. One defines a morphism

$$\varphi_{\mathcal{L}} : A \to \check{A} = \mathrm{Pic}^0_{A/R}$$

by setting

$$x \mapsto \langle T_x^* \mathcal{L} \otimes \mathcal{L}^{-1} \rangle.$$

The group $\mathrm{Pic}^0_{A/R}$ is representable by an abelian scheme. This follows from the fact that the categories of abelian algebraic spaces and abelian schemes coincide (see [FC90] Ch. I, Theorem 1.9) and $\mathrm{Pic}^0_{A/R}$ is representable by an abelian algebraic space (compare [BLR90] Ch. 8, Theorem 1). We denote the kernel of the morphism $\varphi_{\mathcal{L}}$ by $H(\mathcal{L})$. A line bundle $\mathcal{L}$ on A satisfies $H(\mathcal{L}) = A$ if and only if its class is in $\mathrm{Pic}^0_{A/R}(R)$. Also it is well-known that if $\mathcal{L}$ is relatively ample then $\varphi_{\mathcal{L}}$ is an isogeny. In the latter case we say that $\mathcal{L}$ has degree d if $\varphi_{\mathcal{L}}$ is fiber-wise of degree d. Let S be an R-algebra. We define

$$G(\mathcal{L})(S) = \left\{ \ (x,\varphi) \ \mid \ x \in H(\mathcal{L})(S), \ \ \varphi : \mathcal{L}_S \xrightarrow{\sim} T_x^* \mathcal{L}_S \ \right\}.$$

This functor is a group with respect to the group law

$$\big((y,\psi),(x,\varphi)\big) \mapsto (x+y, T_x^*(\psi) \circ \varphi).$$

There is a natural morphism $\pi : G(\mathcal{L}) \to H(\mathcal{L})$ given by $(x,\varphi) \mapsto x$. We get a central exact sequence of fppf-sheaves

$$0 \to \mathbb{G}_{m,R} \to G(\mathcal{L}) \xrightarrow{\pi} H(\mathcal{L}) \to 0. \tag{4.2}$$

Now let $\mathcal{L}$ be relatively ample of degree d. Then $H(\mathcal{L})$ is finite locally free of order d^2 and hence $G(\mathcal{L})$ is a theta group. The commutator pairing on $H(\mathcal{L})$ as defined above will be denoted by $e_{\mathcal{L}}$. One can show that the pairing $e_{\mathcal{L}}$ is perfect, which is equivalent to the fact that the center of $G(\mathcal{L})$ equals $\mathbb{G}_{m,R}$.

4.3.2 Descent of line bundles along isogenies

Let R be a ring. Let $I : A \to B$ be an isogeny of abelian schemes over R and K its kernel. Assume we are given a relatively ample line bundle $\mathcal{L}$ on A and $K \subseteq H(\mathcal{L})$. Define G' by the commutative diagram

$$\begin{tikzcd}
0 \arrow[r] & \mathbb{G}_{m,R} \arrow[r] & G(\mathcal{L}) \arrow[r] & H(\mathcal{L}) \arrow[r] & 0 \\
0 \arrow[r] & \mathbb{G}_{m,R} \arrow[r] \arrow[u, "\mathrm{id}"] & G' \arrow[r, "\pi"] \arrow[u] & K \arrow[r] \arrow[u, hook, "i"'] & 0,
\end{tikzcd} \tag{4.3}$$

where the second row is the pull back of the first via the inclusion $K \overset{i}{\hookrightarrow} H(\mathcal{L})$, i.e. the right hand square is Cartesian. Let S be an R-algebra and $\mathcal{M}$ a line bundle on B_S. Suppose we are given an isomorphism $\alpha : I_S^*\mathcal{M} \xrightarrow{\sim} \mathcal{L}_S$. We define a morphism $s_\alpha : K_S \to G'_S$ by mapping $x \in K(S')$, where S' is an S-algebra, to

$$\big(x, T_x^*(\alpha_{S'}) \circ \alpha_{S'}^{-1}\big).$$

This is well-defined because $T_x^*(I_{S'}^*\mathcal{M}_{S'}) = I_{S'}^*\mathcal{M}_{S'}$. It is clear that $\pi_S \circ s_\alpha = \mathrm{id}$, where π is as in diagram (4.3). We define

$$\underline{\mathrm{Sect}}_K(S) = \{\ s : K_S \to G'_S \ \mid\ \pi_S \circ s = \mathrm{id}\ \}$$

and denote by

$$\underline{\mathrm{Desc}}(\mathcal{L})(S)$$

the set of isomorphism classes of line bundles $\mathcal{M}$ on B_S such that $I_S^*\mathcal{M} \cong \mathcal{L}_S$. The following classical result about descent was proven by A. Grothendieck.

Proposition 4.3.2 *Mapping*

$$(\mathcal{M}, \alpha) \mapsto s_\alpha$$

gives an isomorphism of functors

$$\underline{\mathrm{Desc}}(\mathcal{L}) \to \underline{\mathrm{Sect}}_K.$$

Compare [Mum70] Ch. IV, §23, Theorem 2 or [BLR90] Ch. 6.1, Theorem 4.

4.3.3 Theta structures

In the following we define the standard theta group of a given type. Let K be an a commutative finite locally free group of square order over a base ring R. We set

$$H(K) = K \times_R K^D, \quad G(K) = \mathbb{G}_{m,R} \times_R H(K),$$

and define a group law for $G(K)$ by

$$(\alpha_1, x_1, l_1) * (\alpha_2, x_2, l_2) = (\alpha_1 \cdot \alpha_2 \cdot l_2(x_1), x_1 + x_2, l_1 \cdot l_2).$$

We have an exact sequence of groups

$$0 \to \mathbb{G}_{m,R} \to G(K) \to H(K) \to 0,$$

where the right hand map is the natural projection on $H(K)$. The center of G_K is given by $\mathbb{G}_{m,R}$. Hence $G(K)$ is a theta group. We denote the corresponding commutator pairing by $e(K)$. Using the definition of the multiplication in $G(K)$ one computes

$$e(K)\big((x_1, l_1), (x_2, l_2)\big) = \frac{l_2(x_1)}{l_1(x_2)}. \tag{4.4}$$

We remark that $e(K)$ is a perfect pairing. Now assume we are given an abelian scheme A over R and a relatively ample line bundle $\mathcal{L}$ on A.

Definition 4.3.3 *A* theta structure *of type K for the pair $(A, \mathcal{L})$ is an isomorphism $\theta : G(K) \xrightarrow{\sim} G(\mathcal{L})$ making the diagram*

$$\begin{tikzcd} \mathbb{G}_{m,S} \arrow[r] & G(\mathcal{L}) \\ \mathbb{G}_{m,S} \arrow[r] \arrow[u, "\mathrm{id}"] & G(K) \arrow[u, "\theta"] \end{tikzcd}$$

commutative. Here the horizontal arrows are the natural inclusions.

Next we want to give another characterization of a theta structure.

Definition 4.3.4 *A* Lagrangian decomposition *for $H(\mathcal{L})$ of type K is an isomorphism*

$$\delta : H(K) \xrightarrow{\sim} H(\mathcal{L}),$$

which is compatible with the commutator pairings $e_{\mathcal{L}}$ resp. $e(K)$ on $H(\mathcal{L})$ resp. $H(K)$.

Let δ be a Lagrangian decomposition for $H(\mathcal{L})$ of type K. We can consider K and K^D as subgroups of $H(\mathcal{L})$ via δ. Assume we are given a pair (u, v) where u resp. v is a section of the pullback of the extension

$$0 \to \mathbb{G}_{m,R} \to G(\mathcal{L}) \xrightarrow{\pi} H(\mathcal{L}) \to 0 \tag{4.5}$$

via the inclusion $K \hookrightarrow H(\mathcal{L})$ resp. $K^D \hookrightarrow H(\mathcal{L})$. We define a morphism $\theta_{u,v} : G(K) \to G(\mathcal{L})$ by

$$\theta_{u,v}(\alpha, x, l) = \alpha \cdot v(l) \cdot u(x).$$

Proposition 4.3.5 *The map*

$$(\delta, u, v) \mapsto \theta_{u,v} \tag{4.6}$$

gives a bijection between the set of triples as above and the set of theta structures for $(A, \mathcal{L})$ of type K.

Proof. First we have to show that the map (4.6) is well-defined. We claim that $\theta_{u,v}$ is a theta structure of type K for $(A, \mathcal{L})$. We have

$$\begin{aligned} &\theta_{u,v}\big((\alpha_1, x_1, l_1) * (\alpha_2, x_2, l_2)\big) \\ &\quad = \alpha_1 \cdot \alpha_2 \cdot l_2(x_1) \cdot v(l_1) \cdot v(l_2) \cdot u(x_1) \cdot u(x_2). \end{aligned}$$

By the definition of the pairing $e_{\mathcal{L}}$ we have

$$v(l_2) \cdot u(x_1) = e_{\mathcal{L}}\big(\delta(l_2), \delta(x_1)\big) \cdot u(x_1) \cdot v(l_2).$$

Since δ is a Lagrangian decomposition we have

$$e_{\mathcal{L}}\big(\delta(l_2), \delta(x_1)\big) = e(K)\big((0, l_2), (x_1, 1)\big) = \frac{1}{l_2(x_1)}.$$

The right hand equality follows by (4.4). This proves that $\theta_{u,v}$ is a morphism of groups. Clearly $\theta_{u,v}$ is $\mathbb{G}_{m,R}$-equivariant.

Next we prove that $\theta_{u,v}$ is an isomorphism by giving an inverse. Let g be a point of $G(\mathcal{L})$. Then $\pi(g) = \delta(x_g, l_g)$ for uniquely determined x_g in K and l_g in K^D. Here π is the projection map of the extension (4.5). Now g and $\theta_{u,v}(1, x_g, l_g)$ both lift $\delta(x_g, l_g)$. Hence those two differ by a unique scalar α_g, i.e.

$$g = \alpha_g \cdot \theta_{u,v}(1, x_g, l_g) = (\alpha_g, x_g, l_g).$$

Hence an inverse of $\theta_{u,v}$ is given by the morphism defined by

$$g \mapsto (\alpha_g, x_g, l_g).$$

In order to prove Proposition 4.3.5 it is sufficient to give an inverse of the map (4.6). Assume we are given a theta structure θ of type K for the pair $(A, \mathcal{L})$. The isomorphism θ induces an isomorphism $\delta(\theta) : H(K) \xrightarrow{\sim} H(\mathcal{L})$. By the definition of the commutator pairing it follows that the isomorphism $\delta(\theta)$ is a Lagrangian decomposition. There are two natural sections of the natural projection $G(\mathcal{L}) \to H(\mathcal{L})$ over K resp. K^D given by

$$u(\theta) : (x, 1) \mapsto \theta\big(1, x, 1\big) \quad \text{and} \quad v(\theta) : (0, l) \mapsto \theta\big(1, 0, l\big).$$

Here we consider K and K^D as subgroups of $H(\mathcal{L})$ via $\delta(\theta)$. An inverse of (4.6) is given by

$$\theta \mapsto \big(\delta(\theta), u(\theta), v(\theta)\big).$$

This finishes the proof of the proposition. $\square$

4.4 Descent along lifts of relative Frobenius and Verschiebung

In the following we repeat some facts about the existence of Frobenius lifts and the descent of line bundles along lifts of Frobenius and Verschiebung. Theorem 4.4.1 and 4.4.2 are known to the experts but they are not yet available in the literature. We prove them in Section 4.5.1 and 4.5.2.

Let R be a complete noetherian local ring with perfect residue class field k of characteristic $p > 0$ and A an abelian scheme having ordinary reduction. By Proposition 2.1.1 there exists an abelian scheme $A^{(p)}$ over R and a commutative diagram of isogenies

$$\begin{tikzcd} A \arrow[r, "F"] \arrow[d, "{[p]}"'] & A^{(p)} \arrow[dl, "V"] \\ A & \end{tikzcd} \tag{4.7}$$

such that F_k equals relative Frobenius. The latter condition determines F uniquely. The kernel of F is given by $A[p]^{\mathrm{loc}}$. The condition that F_k equals relative Frobenius means that there exists a commutative diagram

$$\begin{tikzcd}
A_k \arrow[dr, "F_k"] \arrow[drr, bend left, "f_p"] \arrow[ddr, bend right] & & \\
& A_k^{(p)} \arrow[r, "\mathrm{pr}"] \arrow[d] & A_k \arrow[d] \\
& \mathrm{Spec}(k) \arrow[r, "f_p"] & \mathrm{Spec}(k)
\end{tikzcd}$$

where f_p denotes the absolute p-Frobenius, the vertical maps are the structure maps and the square is Cartesian. Let $\mathcal{L}$ be a line bundle on A. We have a natural isomorphism

$$F_k^*(\mathrm{pr}^*\mathcal{L}_k) = f_p^*\mathcal{L}_k \xrightarrow{\sim} \mathcal{L}_k^{\otimes p} \tag{4.8}$$

given by $l \otimes 1 \mapsto l^{\otimes p}$.

Theorem 4.4.1 *Let $\mathcal{L}$ be ample. There exists a line bundle $\mathcal{L}^{(p)}$ on $A^{(p)}$ determined uniquely up to isomorphism by the following two conditions:*

1. $\left(\mathcal{L}^{(p)}\right)_k \cong \mathrm{pr}^*\mathcal{L}_k$,
2. $F^*\mathcal{L}^{(p)} \cong \mathcal{L}^{\otimes p}$.

Moreover, the line bundle $\mathcal{L}^{(p)}$ is ample and has the same degree as $\mathcal{L}$.

A proof of Theorem 4.4.1 is presented in Section 4.5.1. We set $\mathcal{L}_\alpha = \mathcal{L}^{\otimes\alpha}$ for $\alpha = 1, 2$.

Theorem 4.4.2 *If $\mathcal{L}$ is ample and symmetric then there exists an isomorphism*

$$V^*\mathcal{L}_\alpha \xrightarrow{\sim} \left((\mathcal{L}_\alpha)^{(p)}\right)^{\otimes p} \tag{4.9}$$

for

$$\alpha = \begin{cases} 2 & \text{if } p = 2, \\ 1 & \text{if } p > 2. \end{cases}$$

For $p = 2$ and $\alpha = 1$ the isomorphism (4.9) does not always exist. We illustrate this by a counterexample for the case of elliptic curves in Section 4.5.2. A proof of Theorem 4.4.2 will be given in Section 4.5.2.

4.5 The proofs

In this section we prove the statements of Section 4.1 and 4.4.

4.5.1 Proof of Theorem 4.4.1

In the following we prove Theorem 4.4.1. We use the notation of Section 4.4. Let A be an abelian scheme over R having ordinary reduction and $\mathcal{L}$ an ample line bundle on A. Let $K = A[p]^{\mathrm{loc}}$ and let G' be defined by the Cartesian diagram

$$\begin{tikzcd} G(\mathcal{L}^{\otimes p}) \arrow[r] & H(\mathcal{L}^{\otimes p}) \\ G' \arrow[u] \arrow[r] & K. \arrow[u] \end{tikzcd}$$

Remark 4.5.1 *The group G' is commutative.*

Proof. The commutativity of G' is equivalent to the condition that the commutator pairing $e : A[p] \times A[p] \to \mathbb{G}_m$ is trivial on K. Let T be an R-algebra and $x \in K(T)$. Then the map $e(x, \cdot) : K_T \to \mathbb{G}_{m,T}$ is a T-valued point of $K^D \cong \check{A}[p]^{\mathrm{et}}$ where $\check{A}$ denotes the dual abelian scheme. The map $K \to \check{A}[p]^{\mathrm{et}}$ given by $x \mapsto e(x, \cdot)$ is equal to zero since the image of K is connected and hence equals the image of the unit section in $\check{A}[p]^{\mathrm{et}}$ which forms a connected component. □

The main ingredient in the proof of Theorem 4.4.1 is the following result.

Lemma 4.5.2 *The functor $\underline{\mathrm{Sect}}_K$ is a K^D-torsor over R.*

For the definition of $\underline{\mathrm{Sect}}_K$ see Section 4.3.2.

Proof. Clearly the functor $\underline{\mathrm{Hom}}(K, \mathbb{G}_m)$ acts transitively and faithfully on $\underline{\mathrm{Sect}}_K$. Consider the extension

$$0 \to \mathbb{G}_{m,R} \to G' \to K \to 0. \qquad (4.10)$$

We will show that this extension has a section over an fppf-extension of R. The exact sequence (4.10) induces an exact sequence

$$0 \to \mu_p \to G'[p] \to K \to 0. \qquad (4.11)$$

This follows from the Snake Lemma and the exactness of the Kummer sequence. By Remark 4.5.1 the group $G'[p]$ is commutative. Hence we can apply Cartier duality. Dualizing the exact sequence (4.11) we get an exact sequence

$$0 \to K^D \to G'[p]^D \xrightarrow{\pi} \mathbb{Z}/p\mathbb{Z} \to 0. \tag{4.12}$$

The group $G'[p]^D$ is a K^D-torsor over $\mathbb{Z}/p\mathbb{Z}$ via π. By descent (see [DG70] Ch. III, §4, Prop. 1.9) we conclude that $G'[p]^D$ is finite locally free and hence has a point of order p over an fppf-extension $R \to R'$. As a consequence (4.10)–(4.12) have a splitting over R'. □

Corollary 4.5.3 *The functor* $\underline{\mathrm{Sect}}_K$ *is representable by a finite étale scheme.*

Proof. The representability by a finite locally free R-scheme follows from Lemma 4.5.2 and [DG70] Ch. III, §4, Prop. 1.9. Since A has ordinary reduction, we have $\underline{\mathrm{Hom}}_R(K, \mathbb{G}_m) \cong \check{A}[p]^{\mathrm{et}}$ where $\check{A}$ denotes the dual of A (compare Lemma 2.4.5). It follows by descent that $\underline{\mathrm{Sect}}_K$ is étale. □

Now we can complete the proof of Theorem 4.4.1. We have already seen that there exists a k-rational point x of $\underline{\mathrm{Sect}}_K$ given by the isomorphism (4.8). By Corollary 4.5.3 and the theory of finite étale schemes over Henselian local rings there is a unique R-rational point of $\underline{\mathrm{Sect}}_K$ reducing to the k-rational point x. The first part of the claim of Theorem 4.4.1 now follows from Proposition 4.3.2.

The second part of the claim states that the line bundle $\mathcal{L}^{(p)}$ is ample and of the same degree as $\mathcal{L}$. It suffices to verify the claim on the special fiber since the degree does not jump in a flat connected family. We remark that an abelian scheme over a connected base is connected. It is obvious from the construction that $\mathcal{L}_k^{(p)}$ is ample and has the same degree as $\mathcal{L}_k$. This finishes the proof of Theorem 4.4.1.

4.5.2 Proof of Theorem 4.4.2

First we prove Theorem 4.4.2 in the case $R = k$. Let A be an abelian variety over k and $\mathcal{L}$ a symmetric line bundle on A. We set $\mathcal{L}_\alpha = \mathcal{L}^{\otimes \alpha}$ for $\alpha = 1, 2$.

Proposition 4.5.4 *We have*

$$V^*\mathcal{L}_\alpha \cong \left((\mathcal{L}_\alpha)^{(p)} \right)^{\otimes p}$$

for

$$\alpha = \begin{cases} 2 & \text{if } p = 2, \\ 1 & \text{if } p > 2. \end{cases}$$

Note that we have not assumed that A is ordinary!

Proof. The line bundle

$$\mathcal{L}' = V^*\mathcal{L} \otimes \left(\mathcal{L}^{(p)}\right)^{\otimes -p}$$

is in $\mathrm{Pic}^0_{A^{(p)}/k}$. In order to prove the proposition we have to show that $\mathcal{L}'$ is trivial. By the symmetry of $\mathcal{L}$ we conclude that

$$F^*(V^*\mathcal{L}) \cong [p]^*\mathcal{L} \cong \mathcal{L}^{\otimes p^2}. \tag{4.13}$$

Together with Theorem 4.4.1 this implies that $F^*\mathcal{L}'$ is trivial on A. This means that $\mathcal{L}'$ is in the kernel of the dual

$$\check{F} = \mathrm{Pic}^0_{A/R}(F)$$

of F. The group $\mathrm{Ker}(\check{F})$ is the Cartier dual of $\mathrm{Ker}(F)$ and hence is annihilated by the isogeny $[p]$. As a consequence $\mathcal{L}'$ has order dividing p. Since we have assumed $\mathcal{L}$ to be symmetric, it follows by the definition of $\mathcal{L}^{(p)}$ that

$$[-1]^*\mathcal{L}^{(p)} \cong \mathcal{L}^{(p)}. \tag{4.14}$$

This implies that $\mathcal{L}'$ is symmetric, which is equivalent to

$$\langle \mathcal{L}' \rangle \in \mathrm{Pic}^0_{A/R}[2](k)$$

where $\langle \cdot \rangle$ denotes the class in $\mathrm{Pic}^0_{A/R}$. By the above discussion the element $\langle \mathcal{L}' \rangle$ has order dividing the greatest common divisor of p and 2. If $p > 2$, we conclude that $\mathcal{L}'$ is trivial. If $p = 2$, then

$$\left(\mathcal{L}'\right)^{\otimes 2} = V^*\mathcal{L}_2 \otimes \left(\mathcal{L}_2^{(2)}\right)^{\otimes -2}$$

is trivial. This proves the proposition. $\square$

Counterexample $p = 2$, $\alpha = 1$: We assume k to be algebraically closed. Let E be an ordinary elliptic curve over k and $Q \in E^{(2)}[2](k)$ a generator of the kernel of Verschiebung $V : E^{(2)} \to E$. We have

$$V^*(0_E) = (0_{E^{(2)}}) + (Q) \not\sim 2 \cdot (0_{E^{(2)}}),$$

where 0_E resp. $0_{E^{(2)}}$ denote the zero sections of E resp. $E^{(2)}$ and $\sim$ stands for linear equivalence of Weil divisors.

Now we switch to the notation of Section 4.4. The ring R is assumed to be complete noetherian local with perfect residue class field k of characteristic $p > 0$. Assume we are given an abelian scheme A over R having ordinary reduction and an ample symmetric line bundle $\mathcal{L}$ on A. Let

$$\alpha = \begin{cases} 2 \text{ if } p = 2, \\ 1 \text{ if } p > 2, \end{cases}$$

and $\mathcal{L}_\alpha = \mathcal{L}^{\otimes \alpha}$. We set

$$\mathcal{L}' = V^* \mathcal{L}_\alpha \otimes \left(\mathcal{L}_\alpha^{(p)} \right)^{\otimes -p}.$$

Let G denote the kernel of the dual $\check{F} = \mathrm{Pic}^0_{A/R}(F)$ of F. Reasoning as in the proof of Theorem 4.5.4 one shows that $\mathcal{L}'$ gives an R-rational point x of G. Since A has ordinary reduction the kernel of F is toroidal. We have $G^D = \mathrm{Ker}(F)$ and hence G is étale. By Proposition 4.5.4 the point x reduces to zero. By the étaleness of G we conclude that x itself is equal to zero. This proves Theorem 4.4.2.

4.5.3 Proof of Theorem 4.1.1 and Corollary 4.1.2

We use the notation of Section 4.1. Let A be an abelian scheme of relative dimension g over R having ordinary reduction and $\mathcal{L}$ an ample line bundle of degree 1 on A.

First we prove Theorem 4.1.1. Let $K = (\mathbb{Z}/p\mathbb{Z})^g_R$. As a first step we will construct a Lagrangian decomposition

$$K \times_R K^D \xrightarrow{\sim} H\left(\left(\mathcal{L}^{(p)} \right)^{\otimes p} \right) = A^{(p)}[p]$$

depending on the isomorphism (4.1). In a second step we will show that this Lagrangian decomposition is part of a natural theta structure of type K for the pair

$$\left(A^{(p)}, \left(\mathcal{L}^{(p)} \right)^{\otimes p} \right).$$

Assume we are given an isomorphism

$$(\mathbb{Z}/p\mathbb{Z})^g_k \xrightarrow{\sim} A_k[p]^{\mathrm{et}}. \tag{4.15}$$

The reduction functor gives an equivalence of the categories of finite étale groups over R and of finite étale groups over k. Hence the isomorphism (4.15) determines in a unique way an isomorphism

$$K \xrightarrow{\sim} A[p]^{\mathrm{et}}. \tag{4.16}$$

The isogeny $F : A \to A^{(p)}$ induces a commutative diagram

$$\begin{tikzcd}
0 \arrow[r] & A[p]^{\mathrm{loc}} \arrow[r] \arrow[d, "F[p]^{\mathrm{loc}}"] & A[p] \arrow[r] \arrow[d, "F[p]"] & A[p]^{\mathrm{et}} \arrow[r] \arrow[d, "F[p]^{\mathrm{et}}"] & 0 \\
0 \arrow[r] & A^{(p)}[p]^{\mathrm{loc}} \arrow[r] & A^{(p)}[p] \arrow[r] & A^{(p)}[p]^{\mathrm{et}} \arrow[r] & 0
\end{tikzcd}$$

where $F[p]^{\mathrm{et}}$ is an isomorphism (compare Lemma 2.5.2). Composing the isomorphism (4.16) with $F[p]^{\mathrm{et}}$ we get an isomorphism

$$m : K \xrightarrow{\sim} A^{(p)}[p]^{\mathrm{et}}. \tag{4.17}$$

The isomorphism $F[p]^{\mathrm{et}}$ induces a unique section

$$r : A^{(p)}[p]^{\mathrm{et}} \to A^{(p)}[p]$$

of the natural projection $A^{(p)}[p] \to A^{(p)}[p]^{\mathrm{et}}$. We define $t = r \circ m$. For ease of notation we set

$$H = A^{(p)}[p], \quad C = A^{(p)}[p]^{\mathrm{loc}} \quad \text{and} \quad E = A^{(p)}[p]^{\mathrm{et}}.$$

Let $e(\cdot, \cdot)$ denote the commutator pairing on

$$H = H\left(\left(\mathcal{L}^{(p)}\right)^{\otimes p}\right).$$

Since e is a perfect pairing, it induces an isomorphism

$$\varphi : H \xrightarrow{\sim} H^D, \ \ x \mapsto e(x, \cdot).$$

Since C is connected, the isomorphism φ maps C to the connected component of H^D. As a matter of fact the connected component of H^D is given by E^D (compare Lemma 2.4.5), and the isomorphism φ induces isomorphisms

$$\alpha : C \xrightarrow{\sim} E^D \quad \text{resp.} \quad \beta : E \xrightarrow{\sim} C^D$$

on the local resp. étale part of H. We define

$$k = -(\alpha^{-1} \circ m^{-D}) : K^D \xrightarrow{\sim} C,$$

and set $s = i \circ k$.

Lemma 4.5.5 *The morphism $\delta = s \oplus t$ is a Lagrangian decomposition of type K for H.*

Proof. Consider the commutative diagram

$$\begin{tikzcd}
K^D \arrow[r, "k"] \arrow[d] \arrow[dr, "s"] & C \arrow[r, "\alpha"] \arrow[d, "i"] & E^D \arrow[r, "m^D"] \arrow[d, "p^D"] & K^D \arrow[d] \\
K \times K^D \arrow[r, "\delta"] \arrow[d] & H \arrow[r, "\varphi"] \arrow[d, "p"] & H^D \arrow[r, "\delta^D"] \arrow[d, "i^D"] & K \times K^D \arrow[d] \\
K \arrow[r, "m"] \arrow[ur, "t"] & E \arrow[r, "\beta"] & C^D \arrow[r, "k^D"] & K.
\end{tikzcd}$$

By definition we have

$$m^D \circ \alpha \circ k = -\mathrm{id}.$$

Since the pairing e is alternating, we have $\varphi^D = -\varphi$. This implies that $\beta^D = -\alpha$. Hence

$$k^D \circ \beta \circ m = \big(m^D \circ (-\alpha) \circ k\big)^D = \mathrm{id}.$$

The commutator pairing $e(K)$ on $K \times K^D$ gives an isomorphism

$$\tau : K \times K^D \to K \times K^D,\ \ z \mapsto e(K)\big(z, \cdot\big).$$

One computes

$$\tau\big((x,l)\big) = (x, l^{-1}).$$

As a consequence

$$\tau = \delta^D \circ \varphi \circ \delta,$$

which proves that δ is compatible with the natural commutator pairings on H and $K \times K^D$. $\square$

Now the image of K under δ is by construction the kernel of the lift of Verschiebung $V : A^{(p)} \to A$. For the definition of V see Section 4.4. If we combine Theorem 4.4.1 and Theorem 4.4.2 with Proposition 4.3.2, then we get sections

$$u : K \to G\left(\left(\mathcal{L}^{(p)}\right)^{\otimes p}\right) \quad \text{and} \quad v : K^D \to G\left(\left(\mathcal{L}^{(p)}\right)^{\otimes p}\right)$$

of the natural projection

$$G\left(\left(\mathcal{L}^{(p)}\right)^{\otimes p}\right) \to H.$$

Here K and K^D are considered as subgroups of H via the level structure δ constructed above. By Proposition 4.3.5 the triple (δ, u, v) gives a theta structure of type K for the pair

$$\left(A, \left(\mathcal{L}^{(p)}\right)^{\otimes p}\right).$$

This finishes the proof of Theorem 4.1.1.

It remains to prove Corollary 4.1.2. Let $\#k = q = p^d$. Assume now that A is the canonical lift of A_k. As a consequence there exists a unique isomorphism

$$A^{(q)} \xrightarrow{\sim} A$$

such that composing with F^d is an endomorphism of A lifting the absolute q-Frobenius. Applying Theorem 4.1.1 with $A = A^{(p^{d-1})}$ and $\mathcal{L} = \mathcal{L}^{(p^{d-1})}$ we get a natural theta structure of type $(\mathbb{Z}/p\mathbb{Z})^g_R$ for the pair

$$\left(A, \mathcal{L}^{\otimes p}\right).$$

This completes the proof of Corollary 4.1.2.

Bibliography

[BLR90] Siegfried Bosch, Werner Lütkebohmert, and Michel Raynaud. *Néron models*. Number 21 in Ergebnisse der Mathemathik, 3. Folge. Springer-Verlag, 1990.

[DG70] Michel Demazure and Pierre Gabriel. *Groupes Algébriques, Tome I*. North-Holland Publishing Company, Amsterdam, 1970.

[FC90] Gerd Faltings and Ching-Li Chai. *Degeneration of abelian varieties*. Number 22 in Ergebnisse der Mathematik, 3. Folge. Springer-Verlag, 1990.

[MB85] Laurent Moret-Bailly. *Pinceaux de variétés abéliennes*, volume 129 of *Astérisque*. Société Mathématiques de France, 1985.

[Mum66] David Mumford. On the equations defining abelian varieties I. *Inventiones Mathematicae*, 1:287–354, 1966.

[Mum70] David Mumford. *Abelian varieties*. Oxford University Press, London, 1970.